Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Блокировка USB-накопителей через GPO: наша методика внедрения

Device Installation Restrictions, белый список VID/PID, BitLocker To Go и аудит событий 6416

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Сотрудник с флешкой выносит базу 1С, клиентские документы и договоры за минуты — мимо почтовых фильтров, прокси и антивируса, без единого следа в логах. Мы закрываем этот канал штатными средствами Windows: GPO Device Installation Restrictions с белым списком корпоративных носителей, BitLocker To Go и PnP-аудитом — без покупки DLP, на парках от 5 до 50 машин.

Почему это важно бизнесу

- Утечка клиентской базы к уходящему сотруднику — прямая потеря выручки; доказать и вернуть данные практически невозможно
- Персональные данные (клиники, бухгалтерии, юрфирмы) — штрафы по 152-ФЗ и проверки при инциденте
- Стоимость решения — часы инженера и партия флешек; DLP на 30 рабочих мест — сотни тысяч рублей ежегодно
- Чужая флешка — ещё и канал заноса шифровальщика в обход периметра; восстановление — дни простоя

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

6416

код события «внешнее устройство распознано системой» — пишется и по заблокированным попыткам

Audit PNP Activity, журнал Security

1809+

Windows 10 с CU 2021 (KB5005102/KB5004296): layered-политика — allow по VID/PID перекрывает об...

Policy CSP — DeviceInstallation

90+30 мин

фоновое применение GPO: 90 минут плюс случайное смещение до 30; на пилоте — gpupdate /force и...

наш стандарт + доки Group Policy

без REV

формат ID в белом списке: USB\VID_xxxx&PID_xxxx — покрывает всю партию независимо от прошивки

наш стандарт

4663

Audit Removable Storage: чтение/запись на носителях; отказ — 4656, нужен ещё Audit Handle Mani...

по докам learn.microsoft.com

24 ч

интервал коллектора Get-WinEvent: события 6416/4663 со всего парка, сводка на почту админу

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Запрет носителей: Device Installation Restrictions

Что настраиваем

Все рабочие станции домена — GPO ITF_USB_Lockdown на OU Workstations; серверы и ПК админов — в отдельной OU со своей политикой

Как мы это делаем

1. Включаем «Prevent installation of removable devices» (Система → Установка устройств → Ограничения на установку устройств) с флагом «применять к уже установленным»
2. На Windows 10 (1809+ с CU 2021) и Windows 11 включаем «Apply layered order of evaluation»: иерархия instance ID → device ID → setup class → removable
3. Снимаем ID корпоративной партии: Get-PnpDevice -PresentOnly | Where-Object InstanceId -like 'USB\VID_*' либо devmgmt.msc → Сведения → ИД оборудования
4. Белый список: «Allow installation of devices that match any of these device IDs» — USB\VID_xxxx&PID_xxxx всей партии
5. Проверяем применение: gpupdate /force, ветка HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions и секция «Device Installation Restrictions Policy C...

РЕЗУЛЬТАТ

Чужие носители не устанавливаются вообще — пользователь видит отказ установки драйвера, корпоративная партия работает штатно. Политика хранится на контроллере домена, из сеанса пользователя не отключается, новые машины получают запрет автоматически при попадании в OU.

КЛЮЧЕВОЙ НЮАНС

По умолчанию Prevent имеет приоритет над Allow — белый список поверх «Prevent removable» надёжен только с layered-политикой (Windows 10 1809+ с CU 2021, Windows 11); на сборках без неё запрещаем по device ID U...

РЕАЛИЗАЦИЯ 2 ИЗ 3

Второй рубеж: RDS, Removable Storage Access, BitLocker To Go

Что настраиваем

Терминальные серверы RDSH и станции, где съёмные носители разрешены белым списком

Как мы это делаем

1. На RDSH включаем «Не разрешать перенаправление дисков» (fDisableCdm=1, Remote Desktop Session Host → Перенаправление устройств) — режем вынос через \\tsclient
2. Removable Storage Access: «Съёмные диски: Запретить запись» и «Запретить выполнение» — контроль доступа работает даже при уже установленном драйвере
3. Включаем «Запретить запись на съёмные диски без защиты BitLocker» (RDVDenyWriteAccess=1) — запись только на шифрованные носители
4. Корпоративную партию шифруем BitLocker To Go, ключи восстановления кладём в AD DS (объекты класса msFVE-RecoveryInformation)

РЕЗУЛЬТАТ

Даже разрешённая флешка бесполезна при краже или потере — содержимое зашифровано; запись мимо шифрования невозможна, запуск исполняемых файлов со съёмных дисков запрещён, а канал выноса через проброс локальных дисков RDP закрыт на уровне сервера.

КЛЮЧЕВОЙ НЮАНС

Три независимых слоя: Device Installation — установка драйвера, Storage Access — доступ, BitLocker — содержимое. Блокировка только на RDS-сервере без fDisableCdm бесполезна — данные уходят через проброшенный д…

РЕАЛИЗАЦИЯ 3 ИЗ 3

Аудит подключений и ежедневная сводка

Что настраиваем

Все машины домена + сервер с PowerShell-коллектором; журнал Security — единственный источник фактов

Как мы это делаем

1. Advanced Audit Policy → Подробное отслеживание → «Audit PNP Activity» (Success): каждое подключение пишет 6416 с Hardware ID, именем устройства и машиной; запрет ус…
2. Доступ к объектам → «Audit Removable Storage»: 4663 фиксирует чтение/запись файлов; для событий отказа 4656 дополнительно включаем Audit Handle Manipulation (Failur…
3. Включаем «Audit: Force audit policy subcategory settings» (SCENoApplyLegacyAuditPolicy=1) — иначе старые категории затирают подкатегории
4. Увеличиваем журнал Security до 512 МБ на станциях — при штатных 20 МБ события живут считанные дни
5. Коллектор: Get-WinEvent -FilterHashtable @{LogName='Security';Id=6416,4663} раз в сутки по парку, сводка на почту ответственному

РЕЗУЛЬТАТ

Каждая попытка воткнуть чужой носитель видна: кто, где, когда и какой Hardware ID. Повторяющиеся попытки на разных машинах — сигнал для разговора с сотрудником до инцидента, а не после. Для парка 10–50 машин это заменяет SIEM без ежегодных лицензий.

КЛЮЧЕВОЙ НЮАНС

6416 пишется и для заблокированных устройств, а сам запрет установки фиксирует 6423 — вместе это индикатор попыток обхода; без форс-флага подкатегорий аудит молча не работает — первым делом auditpol /get /cate…

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Deny глушит белый список**
  До layered-политики Prevent removable приоритетнее Allow-ID; включаем «Apply layered order of evaluation» (Win10 1809+ с CU 2021, Win11) или запрещае…

- ✕ **Блокировка класса USB целиком**
  GUID {36FC9E60-C465-11CF-8056-444553540000} — это USB-хабы и контроллеры: ляжет вся периферия; съёмные диски режем отдельной политикой

- ✕ **Локальные админ-права**
  Пользователь-админ вернёт службу USBSTOR (Start=3) или снимет политику; до lockdown выводим всех из локальной группы Administrators

- ✕ **Уже установленные флешки**
  Без флага «применять к уже установленным устройствам» носители, вставлявшиеся раньше, продолжают работать; хвосты чистим pnputil /remove-device

- ✕ **Проброс дисков по RDP**
  Данные уходят через \\tsclient в обход блокировки на сервере; на всех RDSH включаем «Не разрешать перенаправление дисков» (fDisableCdm)

- ✕ **Одинаковые VID/PID у noname**
  Разные модели безымянных флешек делят один VID/PID — белый список их не различит; берём брендовую партию или ID экземпляра с серийником

- ✕ **Токены и составные устройства**
  Рутокен/JaCarta — смарт-карты, под USBSTOR не попадают; составные модели с CCID+накопителем проверяем в devmgmt и вносим в allow заранее

- ✕ **Доки и картридеры USB-C**
  Картридеры доков Dell/Lenovo видны как накопители и блокируются, но встроенные хранилища ведут себя нестандартно — пилот на реальном железе

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- «Prevent installation of removable devices» на OU рабочих станций
- Флаг «применять к уже установленным устройствам» включён
- Рядовые пользователи выведены из локальных администраторов
- Пилот на 1–2 машинах: gpupdate /force, проверка мыши, токенов, принтеров

НОРМАЛЬНО

- Белый список VID/PID корпоративной партии + layered-политика (AllowDenyLayered=1)
- «Не разрешать перенаправление дисков» на всех RDS-хостах
- Audit PNP Activity: события 6416/6423 в журнале Security

ХОРОШО

- BitLocker To Go + запрет записи на диски без BitLocker (RDVDenyWriteAccess)
- Запрет выполнения со съёмных дисков + ключи восстановления в AD DS
- Ежедневная сводка 6416/4663 коллектором Get-WinEvent на почту
- Пароль на UEFI и запрет загрузки с внешних носителей

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- ☐ Политика запрета съёмных устройств применена ко всем станциям — gpresult это подтверждает?
- ☐ Белый список содержит только VID/PID корпоративной партии и проверен реальным устройством?
- ☐ Layered-политика включена (Win10 с CU 2021 / Win11) и allow действительно перекрывает deny?
- ☐ У рядовых сотрудников нет прав локального администратора?
- ☐ Проброс локальных дисков в RDP-сессии запрещён на всех терминальных серверах?
- ☐ Флешки, работавшие до внедрения, реально перестали определяться?
- ☐ Аудит PNP включён и событие 6416 появляется в Security при тестовом подключении?
- ☐ Запись на съёмные диски без BitLocker запрещена, ключи восстановления — в AD?
- ☐ Токены КриптоПро, доки и картридеры проверены на пилотной группе?
- ☐ Ежедневный отчёт о попытках подключения доходит до ответственного?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Развернём USB-lockdown под ключ: GPO, белый список партии, retro-применение, план отката
- Поставим аудит 6416/4663 и ежедневную почтовую сводку по всем машинам парка
- Закроем смежные каналы: RDP-проброс дисков, локальные админ-права, загрузка с внешних носителей
- Зашифруем корпоративные носители BitLocker To Go: ключи в AD, учёт и маркировка партии
- Сопровождение: добавление устройств в белый список и разбор инцидентов в рамках абонентки

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Manage Device Installation with Group Policy (learn.microsoft.com — 2025)

02 Policy CSP — DeviceInstallation (EnableInstallationPolicyLayering) (learn.microsoft.com — 2025)

03 Audit PNP Activity / событие 6416 (learn.microsoft.com — Win10/11)

04 Monitor the use of removable storage devices (learn.microsoft.com — Win10/11)

05 BitLocker Group Policy settings (RDVDenyWriteAccess) (learn.microsoft.com — Win11)

06 Шаблон GPO ITF_USB_Lockdown + PowerShell-коллектор (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.